

Mark Russinovich: Software Whiz, Cybercrime Writer

Hilton Collins | May 24, 2013



[Mark Russinovich](#) looks like an average corporate computer whiz, even though he's a technical fellow for Microsoft. The tall, thin, dark-haired software guru helps co-workers maintain successful products like SQL Server, Visual Studio and the ubiquitous Windows operating system.

His words are measured, calm and occasionally soft-spoken in speeches and conversations, befitting the popular notion that a man who tinkers with technology behind the scenes doesn't need boisterous flair or a dominating presence.

But his unassuming demeanor hides a surprising level of creative intensity. When Russinovich isn't zeroing in on computer problems at work, he uses that same laser-like focus to craft tales of intrigue and espionage as a novelist. He writes techno thrillers from an insider's point of view, pitting fictional computer analysts and government agents against cybercriminals terrorizing society.

His stories paint a vivid, chilling picture of how digital wrongdoing jeopardizes activities that people take for granted. In his first novel, *Zero Day*, illegal hackers nearly cause a nuclear meltdown and disrupt a plane's control system midflight. In his second novel, *Trojan Horse*, state-sponsored cyberespionage infiltrates international networks and threatens global relations.

Each book currently rates an average of more than four stars on Amazon, evidence that Russinovich tells stories with just as much skill as he uses to develop Microsoft

products. The possibility of negative feedback worried him in the beginning, but positive ratings relieved him after [Zero Day](#)'s 2011 debut.

"I tried to set myself up for, 'OK, if I hit three stars, then I'll consider that a success as a first book,'" he said. "And the response has been way more positive than that."

"I tried to set myself up for, 'OK, if I hit three stars, then I'll consider that a success as a first book,'" he said. "And the response has been way more positive than that."

Prescient Prose

Russinovich's tales thrill readers with intense opening scenes illustrating the dangers of cybercrime.

Pilots and nearly 300 passengers of a Boeing 787 Dreamliner are shell-shocked in *Zero Day*'s first chapter when the airliner unexpectedly climbs tens of thousands of feet above the Atlantic Ocean. The jet's hacked computer takes on a life of its own, sending the 787 more than 43,000 feet into the air before stalling in the sky. Occupants panic when they suddenly plummet toward the water below.

In [Trojan Horse](#), terror starts spreading through Yakima, Wash. A malware-infected power grid causes a hospital's electricity to go out during an operation to remove shrapnel from a girl's brain after a car accident. Elsewhere, a power outage stops one train dead on the tracks, while another train barrels toward it from behind. Will the power return in time for the doctor to save his patient? Will the engineer regain control of his train and move it out of the other's path before they collide?

These deadly scenarios plague characters early in Russinovich's novels, and they're striking examples of what illegal hacking may cause in real life. "I think the goal is to scare the government," he said. "The fact is, our nation's critical infrastructure is operated by private industry with very little regulation or oversight by the government."

The American media hasn't reported frightening events of this magnitude yet, but network infiltration grows at an alarming rate. Surprising statistics include the following:

- According to a federal report, companies in charge of the country's critical infrastructure experienced a dramatic increase in attacks on their networks from 2009 to 2011. The government fielded nine incident reports in 2009 and a staggering 198 in 2011 — a 2,200 percent increase.
- In September 2012, a software supplier to Canadian and American electrical systems reported that it had been hacked by Chinese assailants who accessed America's power grid.
- In July 2012, a man exposed weakness in an air traffic control system during a conference demonstration by using \$2,000 worth of store-bought equipment to fool the system into believing that a nonexistent plane was landing.

As a Microsoft employee, Russinovich is well aware that Windows, the world's most-used operating system, is constantly under attack. He raised the issue in a February speech at the 2012 RSA Conference, a popular destination for tech luminaries. Russinovich suggested that the world could be on the verge of the kind of

cyberterrorism his fiction depicts, and he referenced testimony that then-U.S. Sen. Joe Lieberman gave to Congress earlier that month.

The senator likened today's cybervulnerabilities to the physical vulnerabilities that terrorists exploited on 9/11. "To me, it feels like it is Sept. 10, 2001. The system is blinking red, again," Lieberman said. "Yet, we are failing to connect the dots, again."

Russinovich created characters in his stories that are prepared for the worst. Computer security expert Jeff Aiken stars in *Zero Day* and *Trojan Horse*, and he fights criminals and enemy governments. Government agent Daryl Haugen joins him in the mission to protect America, and they handle the worst their adversaries throw at them.

Russinovich weaves drama into his stories with enough technical authority to keep them grounded in reality, and the result is so real it's creepy. Plots thicken once his characters detect malware wreaking havoc. In *Zero Day*, the first investigation pits them against terrorists operating under the *al-Qaida* label who outsource their hacking efforts elsewhere.

"The plot was hung off this scenario I consider a real threat: terrorists realizing the power of cyberweapons, outsourcing it because they don't have the knowledge themselves and carrying out this slow spreading attack on a certain day," he said.

A Technical Foundation

Russinovich's impressive technical background seems atypical for someone with artistic sensibilities. He earned a master's degree in computer engineering from Rensselaer Polytechnic Institute in 1990 before getting his Ph.D. from Carnegie Mellon in 1994.



His ingenuity after graduation caught Microsoft's attention. In 1996, he co-founded Winternals Software, a company offering software to help people manage computers running Windows. Microsoft bought the company in 2006 and hired Russinovich as a technical fellow, his current role. He's also one of

the writers behind the Windows Internals nonfiction series that teaches readers how Windows functions.

Writing cyberthrillers may seem like an odd choice for someone so technical, but it's a natural fit: Who else but a computer whiz would have such a firm grasp on digital drama?

When Russinovich started his novelist career with *Zero Day*, he knew he would expose the insider world of software security and government bureaucracy to readers who may be unfamiliar with its intricacies.

"I was like, 'I'm going to write it for myself, which is a niche kind of audience. I know that audience will probably like it. I have no idea what people outside of that targeted audience will think of it,'" he said.

His risk paid off. Russinovich said in his RSA speech that *Zero Day* had sold tens of thousands of copies, an admirable debut for a first novel. The result gave him and his publisher, Thomas Dunne Books, the confidence to produce *Trojan Horse*, the second Jeff Aiken novel, released in fall 2012. Russinovich also wrote an Aiken short story, *Operation Desolation*, and his third novel in the series, *Rogue Code*, drops in spring 2014.

Surprisingly, being a successful and productive novelist hasn't changed Russinovich's life much, but his friends may see him differently now.

"I think friends don't really know what to think of it. I think they're impressed, but they're bemused because I'm one of them and yet I have this background activity of fiction going on."

Rewarding Journeys

Fiction writing was a natural evolution for Russinovich personally, who's been a science fiction and thriller fan since childhood. He enjoys stories by sci-fi and thriller legends Isaac Asimov and Michael Crichton, and he plays the Battlefield first-person shooter video game series. Russinovich has yearned to tell his own stories for several years.

"Wanting to write fiction is something that's been a thought of mine since I was young," he said. The fact that people used technology as backdrops for exciting adventures fascinated him. "I felt like I was learning something and getting smarter, and yet the story was also entertaining."

The 9/11 tragedy spurred him to write *Zero Day*, which launched his novelist career, but the road to techno thriller proficiency was long. He finished the book in 2006 and spent years searching for a publisher before Thomas Dunne Books released it in 2011.

The journey to publication was stressful and time consuming. When Russinovich decided to write fiction, he expected publishers to be welcoming. He'd already written nonfiction books about software, and his Sysinternals.com website garnered tens of thousands of hits. The thinking was that publishers would be impressed by his background, but things didn't go smoothly.

“I started by emailing a bunch of publishers and didn’t get any answers, so I bought books on getting publishers, and what they really recommend you do is go find an agent,” he said. “I went through three rounds of sending out packages to agents.”

The packages explained why his background made him a viable candidate and included excerpts from the book. Russinovich struck out three times before he found a willing agent, which took more than a year after *Zero Day*’s completion. The agent went through more rounds of submitting similar packages to publishers, and the rejection letters weren’t very informative.

“It’s like, ‘Oh, we’re going to pass at this time,’ or ‘This doesn’t fit with our line-up,’” he said.

“It’s like, ‘Oh, we’re going to pass at this time,’ or ‘This doesn’t fit with our line-up,’” he said.

Russinovich broke through a major barrier when his first novel finally came out, and publishing successive books has been much easier. But one thing that will always require hard work no matter how his career goes is the writing process itself.

He likened creative writing challenges to public speaking challenges he’s faced in the past. “Public speaking was never easy for me. It’s not for a lot of people, and that drew me to it because this is a challenge,” he said. “I [thought], ‘This is hard for me, so I would really love to conquer this, to attack it and get better at it.’ And writing is kind of the same way.”

But overcoming artistic hurdles doesn’t scare Russinovich because he’s a seasoned pro. He has years of experience attacking problems methodically — creative and technical.

“I don’t feel like I’m the genius piano player that can just spit out a masterpiece. I am much more intellectual about what I’m doing, and that’s harder than I think, to somebody who’s natural at it, but it’s also what draws me to it.”

<http://www.govtech.com/security/Mark-Russinovich-Software-Whiz-Cybercrime-Writer.html>